PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
WILLIAM F. AHMANN
PERKINS COIE LLP
101 JEFFERSON DRIVE
MENLO PARK, CA 94025

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	28 MAY 2008
Applicant's or agent's file reference 57159-8017.WO01	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US07/19862	12 September 2007 (12.09.2007)	16 October 2006 (16.10.2006)

International Patent Classification (IPC) or both national classification and IPC

IPC: **H04L 9/00**(2006.01),**9/32**(2006.01);**G06F 11/30**(2006.01),**12/14**(2006.01)
USPC: 713/170,176,177,181,187

Applicant

BROADON COMMUNICATIONS, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I — Basis of the opinion
- ☐ Box No. II — Priority
- ☐ Box No. III — Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV — Lack of unity of invention
- ☒ Box No. V — Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI — Certain documents cited
- ☐ Box No. VII — Certain defects in the international application
- ☐ Box No. VIII — Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis(b)* that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	19 May 2008 (19.05.2008)	SHAHROUZ YOUSEFI Telephone No. 5712722100

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/19862

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:
   - ☒ the international application in the language in which it was filed
   - ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

   a. type of material
      - ☐ a sequence listing
      - ☐ table(s) related to the sequence listing

   b. format of material
      - ☐ on paper
      - ☐ in electronic form

   c. time of filing/furnishing
      - ☐ contained in the international application as filed.
      - ☐ filed together with the international application in electronic form.
      - ☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/19862

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims 1-21	YES
	Claims NONE	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-21	NO
Industrial applicability (IA)	Claims 1-21	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

International application No.
PCT/US07/19862

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

V. 2. Citations and Explanations:
Claims 1-14 and 18-21 lack an inventive step under PCT Article 33(3) as being obvious over Sprunk et al. (US 2005/0071640) hereinafter Sprunk in view of Asano et al. (US 2002/0154779) hereinafter Asano.

1. With respect to claims 1 and 21, Sprunk discloses accessing a header including a data structure and a set of hash values (obtain an initial hash value for a set of information block, fig. 1, element 104); obtaining from the data structure a first root hash of a hierarchical hash tree (par. [0009]); computing a second root hash from the set of hash values (calculating a second hash key, par. [0009]); comparing the first root hash to the second root hash (comparing the check root key with the initial root key, par. [0009]); if the first root hash and the second root has match (accepting the new root key if the check root key matches the initial root key, par. [0009]), obtaining an encrypted key from the data structure (The branch keys are encrypted, par. [0041], fig. 8B, element 832); securely storing the key such that the key is not passed in the clear (store the hash keys for the plurality of blocks of data, fig. 5A, element 512); providing a reference to the key (calculating hash keys for the plurality of blocks of data so that each of the hash keys corresponds to only one of the blocks of the data and so that each of the blocks of data corresponds to only one of the hash keys, par. [0009], fig. 5A, element 508); loading authentication data from a sub-block associated with the data block (authenticate information stored remotely from a processor using a hash algorithm, par. [0020]); identifying, in the authentication data, a first set of hash values associated with a first level of the hierarchical hash tree (First, the processor obtains an initial hash value for a set of N information blocks where N is an integer, as shown in block 104, par. [0020]); computing a cryptographic hash of the data block to determine a first hash value (A revised hash value for the revised set of N information blocks is calculated in block 112, par. [0020]); comparing the first hash value to a corresponding value in the first set of hash values (The check hash value is compared with the initial hash value in block 120, par. [0020]); rejecting a block data request if the first hash value and the corresponding value in the first set of hash values do not match (are the check hash value and the initial hash value identical, fig. 3B, element 352, indicate a failure, fig. 3C element 376, also, par. [0020]). Sprunk does not disclose decrypting the encrypted key. However, Asano discloses securely decrypting the encrypted key (decryption keys to decrypt encrypted contents distributed, par. [0007]); and decrypting a data block with the reference to the key (decrypting the input content block with the content Key, par. [0456]). It would not involve an inventive step to modify Sprunk with the decryption ability of Asano to insure security of save data.
2. With respect to claim 2, Asano discloses the data structure is public key signed par. [0011].
3. With respect to claim 3, Sprunk discloses authenticating the data structure (a method for authenticating a string of data, abstract).
4. With respect to claim 4, Asano discloses securely storing the set of hash values included in the header (the content program's individual encryption keys are the content key Kcon stored in the header unit of the content data including the content program, par.

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/19862

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

[0025]).

5. With respect to claim 5, Sprunk discloses caching the hierarchical hash tree, figure 6 and figure 7.

6. With respect to claim 6, Sprunk discloses rejecting the header if the first root hash and the second root hash do not match, par. [0020].

7. With respect to claim 7, Sprunk discloses validating a rights management ticket from a source other than the header (the set of data for digital rights management has been revised and authenticated as only a revision to the block of data, par. [0027]).

8. With respect to claim 8, Sprunk discloses the reference to the key is provided in the clear (calculating hash keys for the plurality of blocks of data so that each of the hash keys corresponds to only one of the blocks of the data and so that each of the blocks of data corresponds to only one of the hash keys, par. [0009], fig. 5A, element 508).

9. With respect to claim 9, Asano discloses decrypting a data block with the reference to the key further comprises: providing the reference to the key to a secure decryption engine; decrypting the data block such that the key is not passes in the clear, par. [0007] and par. [0456].

10. With respect to claim 10, Asano discloses decrypting at least a portion of the sub-block (fig. 22).

11. With respect to claim 11, Sprunk discloses in each hash block: inserting a calculated hash in an appropriate location; computing the hash of the hash block, par. [0008] and par. [0009].

12. With respect to claim 12, Sprunk discloses if the first hash value matches the corresponding value in the first set of hash values, further comprising: computing a second hash value corresponding to the first set of hash values; identifying, in the authentication data, a second set of hash values associated with a second level of the hierarchical hash tree; comparing the second hash value to a corresponding value in the second set of hash values; rejecting the block data request if the second hash value and the corresponding value in the second set of hash values do not match, par. [0009] and par. [0020].

13. With respect to claim 13, Sprunk discloses if the second hash value matches the corresponding value in the second set of hash values, further comprising: computing a third hash value corresponding to the second set of hash values; identifying, in the authentication data, a third set of hash values associated with a third level of the hierarchical hash tree; comparing the third hash value to a corresponding value in the third set of hash values; rejecting the block data request if the third hash value and the corresponding value in the third set of hash values do not match, par. [0009] and par. [0020].

14. With respect to claim 14, Sprunk discloses if the third hash value matches the corresponding value in the third set of hash values, wherein the set of hash values of the header are a fourth set of hash values, and wherein the fourth set of hash values are associated with a fourth level of the hierarchical hash tree, further comprising: computing a fourth hash value corresponding to the third set of hash values; providing a fourth set of hash values associated with a fourth level of the hierarchical hash tree; comparing the fourth hash value to a corresponding value in the fourth set of hash values; rejecting the block data request if the fourth hash value and the corresponding value in the fourth set of hash values do not match; returning the data block if the fourth hash value and the corresponding value in the fourth set of hash values match, par. [0009] and par. [0020].

15. With respect to claim 18, Asano discloses a system having a means for secure content delivery with block-based media (A record reproducing player and save data processing methods capable of insuring security of save data are provided, abstract), comprising: a secure key store means ; a means for accessing an encrypted key from a header of a block-based media device (Save data is stored in a recording device, encrypted with the use of a program's individual encryption key, e.g., a content key, or a save data encryption key created based the content key, abstract); a means for securely decrypting the encrypted key (a decryption process is conducted on it with the use of the save data decryption key particular to the program, Abstract); Asano doesn't disclose hashing functionality. However, Sprunk disclose a means for securely storing the key in the key store (it is possible to store hashing keys for a significantly long data set, par. [0033]); a means for referencing the key to securely decrypt data blocks of the block-based media device; a means for providing hash values in association with the block-based media device and each data block of the block-based media device (obtaining an initial hash value for each set of N information blocks, par. [0008]). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify Sprunk with the decryption ability of Asano to insure security of save data.

16. With respect to claim 19, a means for aborting block-based media device access if hash values in the header are rejected (indicate a failure, fig. 3C element 376, also, par. [0020].

17. With respect to claim 20, a means for aborting data block access if hash values in the data block are rejected (indicate a failure, fig. 3C element 376, also, par. [0020]).

18. Claim 15 lack an inventive step under PCT Article 33(3) as being obvious over Asano et al. (US 2002/0154779) hereinafter Asano, in view of Karajewski, Jr. et al. (US 5,590,199).

19. With respect to claim 15, Asano discloses a block-based media driver coupled to a security API, wherein, in operation, the block-based media driver accesses a header associated with a block-based media device and extracts authentication data from the header (For instance, the recording device 400 retains in the external memory 402 a content contained in content data, and block information contained as header information of the content data, and a variety of key information, e.g., a content key Kcon; all encrypted, with the use of a recording device's individual key (called "storage key (Kstr)" hereinafter) stored in the internal memory 405 inside the recording device, par. [0191]); a security kernel including the security API, an encryption /decryption engine, and a key store accessible to the security API, wherein, in operation, the encryption/decryption engine decrypts the key, the key is stored in the key store, and the security API returns a reference to the key to the ticket services; wherein, in operation, the ticket services validates the authentication data and returns the reference to the key to the block-based media driver; wherein, in operation, the block-based media driver accesses data blocks of the block-based media device, sends a block decryption request to the security API, and the security kernel decrypts the blocks and validates a hierarchical hash tree associated with the data blocks (an encryption/decryption unit 308 to perform an encryption process, decryption process, creation and check of data for authentication, and generation of random numbers, par. [0164], par. [0165]). Asano doesn't disclose a service ticket. However, Karajewski discloses ticket services coupled to the block-based media driver and the security

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/19862

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

API, wherein, in operation, the ticket services receive the authentication data from the block-based media driver and send a key decryption request to the security API (presents the ticket granting service ticket and an associated authenticator 51 to the ticket granting service running on the KAS 32 to request a ticket for the desired system service 20. The authenticator is encrypted by the smart card 30, col. 6, lines 11-35). It would not involve an inventive step to modify Sprunk with the decryption ability of Asano to insure security of save data.

20. Claims 16-17 lack an inventive step under PCT Article 33(3) as being obvious over Asano et al. (US 2002/0154779) hereinafter Asano, in view of Karajewski, Jr. et al. (US 5,590,199) and further in view of Sprunk et al. (US 2005/0071640) hereinafter Sprunk.

21. With respect to claim 16, Sprunk discloses the header associated with the block-based media device includes a root hash value and a plurality of root-child hash values, fig. 6 and 7.

22. With respect to claim 17, Sprunk discloses the data blocks each include a hash sub-block and a plurality of content data blocks (a set of N information blocks can be authenticated by obtaining an initial hash value for each set of N information blocks, where N is an integer, par. [0008]).

23. Claims 1-21 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.